Claims

1. A method for preventing undesirable activities of Executable Objects via an application, comprising denying to the same application, or one or more of its threads, access to a secured resource if it has previously exhibited Internet behavior and has not met a specific condition for accessing said resource, and denying said application, or one or more of its threads, Internet behavior if, at the time access is sought, it is accessing a secured resource.

2. A method according to claim 1, comprising recording in a memory events representative of Internet behavior, keeping a record of all resources that are to be kept secured and when an application that has previously exhibited Internet behavior attempts to access one such secured resource, denying access to said secured resource, unless:
   a) At least a predetermined period of time has passed since the last Internet behavior; or
   b) It has performed at least a predetermined number of operations after exhibiting Internet behavior; or
   c) Another preset condition has been fulfilled.

3. A method according to claim 2, wherein the preset condition comprises the exercise of control over the execution of downloadables received during Internet behavior, to ensure that no unexecuted downloadable may access the secured resource.

4. A method according to claim 2, wherein the preset condition comprises the analysis of the downloadables to ascertain that there are harmless.

5. A method according to any one of claims 1 to 4, wherein Internet behavior is blocked by disabling the network connection creation.

6. A method according to any one of claims 1 to 4, wherein Internet behavior is blocked by disabling specific protocols.

7. A method according to claim 6, wherein the specific protocols comprise HTTP, FTP, SMTP, or the like communication protocol.

8. A method according to any one of claims 1 to 4, wherein Internet behavior is blocked by disabling the transfer of EOs in the communication protocols.

9. A method according to any one of claims 5 to 8, wherein the access to trusted sites is not disabled.

10. A method according to any one of claims 1 to 4, wherein access to a secured resource is blocked by disabling a thread using a specific system service that is used to access the secured resource.

11. A method according to any one of claims 1 to 10, wherein all sub-threads of a thread that is denied access to a secured resource are also denied access to secured resources.

12. A method according to any one of claims 1 to 10, wherein all sub-threads of a thread that is denied Internet behavior are also denied Internet behavior.

13. Apparatus for preventing undesirable activities of Executable Objects via an application, comprising a memory for storing a record of Internet behavior of a plurality of applications, and means for denying to the same application access to a secured resource if it has previously exhibited Internet behavior and has not met a specific condition for accessing said resource.

14. Apparatus for preventing undesirable activities of Executable Objects via an application, comprising a memory for storing a record of Internet behavior of a plurality of applications, and means for denying said application, or one or more of its threads, Internet behavior if, at the time access is sought, it is accessing a secured resource.

15. A system for preventing undesirable activities of Executable Objects via an application, comprising a computer on which one or more applications are to run, said computer being connectable to the Internet or Intranet or Extranet, said computer being provided with a memory for storing a record of Internet behavior of each of said plurality of applications, and means for denying to the same application access to a secured resource if it has previously exhibited Internet behavior and has not met a specific condition for accessing said resource.

16. A system for preventing undesirable activities of Executable Objects via an application, comprising a computer on which one or more applications are to run, said computer being connectable to the Internet or Intranet or Extranet, said computer being provided with a memory for storing a record of Internet behavior of each of said plurality of applications, and means for denying said application, or one or more of its threads, Internet behavior if, at the time Internet behavior is exhibited, it is accessing a secured resource.

17. A method for preventing undesirable activities of Executable Objects via an application, substantially as described and illustrated.